### Advanced Seminar on China Antitrust

April 2, 2015

# Dawn raids: getting prepared and managing the process in China

Ninette Dodoo



Michael Han

FANGDA PARTNERS 方達津師事務所



# Agenda

- Preparing for a dawn raid
- Managing the process
- Defining roles and functions
- Document review
- Due process
- International cooperation



### Preparation for dawn raids

- Dawn raids: by definition always sudden, unexpected and often traumatic for a company
- Why so important for investigated companies?
  - Major risk issues for companies criminal liability, civil liability, fines, loss of reputation, management time, scope creep, directors disqualification, exclusion from public procurement
  - Inherently multi-national for any sizeable company
  - Complexity of issues, over a long period of time and across multiple phases (investigation / decision, appeal, damages actions)
  - Diverse legal and practical skill sets required
  - Costs of the investigation
  - Negative impact can be managed through careful preparation



### Preparation for dawn raids

- Being prepared
  - Key issues:
    - Enhance efficiency through establishing a well-organized response team
    - "Dawn raid emergency plan" setting out:
      - structure of first response in general terms
      - protocol on roles and responsibilities
      - protocol for in-house decision-making process
      - protocol for exchange of search terms and evidence
      - protocol for responses to press enquiries
      - which lawyers to instruct where
      - which forensic IT team + IT process guidelines
    - Educate and train the team



# Managing the process (1)

- Checking the authority and identifying the scope of the investigation
- Possibility of simultaneous raids at multiple locations
- Dawn raid procedures and response
  - should enable leniency to be addressed during the raid
  - make use of technology to help coordinate the company's response
- Establish communication protocol with officials
- Shadow officials during raid
- Organising the team ideally two separate teams
- Document preservation instructions
- Disputes



# Managing the process (2)

- Answering questions and providing assistance
- Interviews during inspections
- Keeping records notes of interviews; copying what is copied/removed; notes of search terms; notes of conversations with officials; closing note of the raid
- Approach to computer records
  - understanding IT systems
  - documents stored on foreign servers
  - imaging of hard drives
  - encrypted emails and emails sent during the raid
- Risks of not co-operating (obstruction, document destruction, providing misleading information)
  - fines and impact on leniency
- Relevance of privacy and data protection arguments in raid situations



# A typical dawn raid: start of day

	EU	China
No. of attendees	<ul> <li>No minimum requirement, dependent on size of undertaking's premises</li> <li>Officials usually accompanied by national officials, often accompanied by one or two IT specialists</li> </ul>	<ul> <li>Minimum of 2 officials</li> <li>Central officials assisted by local officials</li> <li>IT specialists</li> </ul>
Scope of search	<ul> <li>Decision to open proceedings identifies:</li> <li>parties subject to the proceedings</li> <li>behaviour constituting the alleged infringement to be covered by the investigation, and normally specifies the territory and sector(s) where such behaviour takes place</li> </ul>	<ul> <li>Broadly stated inspection search notice</li> <li>A search warrant from the court is not required</li> </ul>

#### In practice...

- Officials arrive, announce the inspection, verify identification and wait a short period of time for a senior company representative to arrive
- Officials generally do not wait for external lawyers to arrive
- Officials may inspect various departments (e.g., sales, finance) simultaneously



# A typical dawn raid: middle of day

	EU	China
Search power: Documents	<ul> <li>Search for and take copies of documents</li> <li>Request that the company identifies and provide officials with documents</li> <li>(In some cases) seize original documents</li> <li>No requirement to hand over: <ul> <li>legally privileged documents</li> <li>documents outside the scope of investigation</li> </ul> </li> </ul>	<ul> <li>Search for and take copies of documents</li> <li>Request that the company identifies and provide officials with documents</li> <li>Documents requested can be very broad</li> <li>Examine bank accounts of the undertakings</li> <li>No concept of legal privilege</li> </ul>

#### In practice...

• Officials and company discuss raid procedure and conduct: (i) what officials want to see and company's IT extraction; (ii) identify key point of contact; (iii) allocate company personnel and roles (including IP rep) to accompany officials during the search; (iv) ensure detailed record taken of all copies of the material taken



# A typical dawn raid: middle of day

	EU	China
Search power:	<ul> <li>Ask for explanations on facts or documents relating to the subject matter</li> </ul>	<ul> <li>Ask for explanations on circumstances relating to the subject matter</li> </ul>
Interview	<ul> <li>May also carry out more general interview subject to individual consents</li> </ul>	
	<ul> <li>Limitation</li> </ul>	
	<ul> <li>privilege against self-incrimination</li> </ul>	

#### In practice...

- Officials may require one-on-one interview and no third party (including the Company's outside counsel) is allowed to attend the interview
- Interviewees will need to sign the interview notes taken by officials (interviewees
  are permitted to review the interview notes before signing), but the Company may
  not be allowed to make a copy of the interview notes



# A typical dawn raid: middle of day

	EU	China
Search power: IT	To examine the books and other records  irrespective of the medium on which they are  stored; to take or obtain in any form copies or extracts  • Access and search IT environment and storage media (e.g. laptops, desktops, tablets, mobile phones, CD-ROM, servers)	<ul> <li>Inspecting and copying relevant documents and materials such as electronic data</li> <li>Currently no published guidance on IT records</li> </ul>
	<ul> <li>Block e-mail accounts, disconnect running computers and (in some cases) seize IT equipment, including mobile phones and blackberries</li> </ul>	
	<ul> <li>Download records of phone calls, voicemails, faxes sent/received</li> </ul>	

- Implications in practice...
  - Increasingly sophisticated methods of electronic recovery officials may bring IT specialists with them
  - Search terms used for emails search
  - Taking forensic "images" of hard disks and servers
  - Authorities may seize laptop/hard drives
  - Servers outside the jurisdiction (and impact of data protection law)?



### A typical dawn raid: end of day

- In practice...
  - Officials indicate whether they will be coming back the next day
  - Check and agree the list of documents copied or seized by the officials
  - Sign the minutes of inspection and the list of documents removed
    - ensure any disputed documents are identified
    - ensure any negotiated concessions made with the authorities are minuted
    - If inspections is to continue the next day, officials may seal relevant spaces and/or materials



### Defining roles and functions

#### **INVESTIGATION COORDINATOR**

- Contact external counsel
- Provide strategic legal advice
- Assess liability and leniency
- Liaise with senior management and PR/GR
- Communicate with the rest of the company
- Deal with escalated disputes
- Provide remote support to site coordinators

#### **CONFERENCE LINE**

- Coordinate response to dawn raid
- Ensure consistency across sites
- Legal advice for difficult issues

#### SITE COORDINATOR

- Contact local external counsel
- Manage response team members
- Point of contact for enforcers
- Coordinate IT support
- Oversee documents provided to investigators

Several Site Coordinators may be needed in multi-site raids

#### **EXTERNAL COUNSEL**

- Assist the Site Coordinator
- Provide legal advice
- Attend the dawn raid
- Deal with escalated disputes
- Prepare report of dawn raid
- Shadowing (if needed)
- Attend interviews (where possible)

#### **RECEPTION/SECURITY**

- Contact Site Coordinator
- Register enforcers
- Guide enforcers

#### **INVESTIGATION SECRETARY**

- Provide admin support for the Site Coordinator and other response team members
- Set up rooms as required
- Logistical support

#### **SHADOWERS** (if needed)

- Keep a detailed record of documents accessed and questions asked/answers given
- In particular, check the search terms and take precise notes of what is being searched

#### IT COORDINATOR

- Liaise with investigators to coordinate information requests and explain company's IT infrastructure
- Facilitate requests for access control and information collection
- Preserve business continuity where possible



# Key phases of lawyer / enforcer interaction

#### (1) Before dawn raids

Leniency application

#### (2) During dawn raids

- Lawyers will shadow officials
- Agreeing on scope of search (incl. e-search terms)
- Coordinating the authority's requests
- Negotiations re leniency
- Both sides should seek to build trust/avoid any confrontational relationship

### (3) Post dawn raid situation assessment

- Negotiations re leniency
- Negotiations re scope of investigation
- Managing information requests and negotiating their scope



### Effective interactions with enforcers

- Build up working relationships and the trust of both sides
  - Be open rather than confrontational
  - Be fair and reasonable
  - Act (and react) predictable, reliable and trustworthy
  - Be transparent as to process and timing, where possible
  - Treat each other with respect and as reliable counterparts
  - Be friendly but professional and firm where necessary



# Advantages of effective interaction (1)

- Incentives for effective interaction on both sides
  - For enforcers: reducing investigation work and fostering investigation success without involving risks for enforcers
    - Investigation becomes easier and more effective
    - Cooperation is voluntary on both sides
    - Sharing preliminary thoughts on certain issues or infringement theories is not binding and based on common understanding that it will not be used against the enforcers
    - Company's outside counsel may help the interaction between enforcers and clients
      - Direct contact with the company's senior management and GC
      - Objective view on legal assessment and risks (combined with experience)
      - More trusted by clients than the enforcers
      - Thus, may smoothen the communication/interaction



# Advantages of effective interaction (2)

- Incentives for effective interaction on both sides
  - For lawyers: fostering representation in investigation and/or leniency
    - Reducing the scope of investigation by sharing and discussing theories or aspects of case
    - Ensuring adequate scope of leniency through further internal investigations and enlarging leniency where necessary
    - Increasing lawyers' standing vis-a-vis their clients if lawyers have working relationship with enforcers and receive additional value (which, in turn, increases cooperation with enforcers)
    - Additional incentives due to repeat play (lawyers interact with enforcers repeatedly)
  - For companies: investigation is better, quicker and cheaper
  - For all: reciprocity (quid pro quo)





### Some Dos and Don'ts

### **DO**



- When dealing with officials:
  - Be calm, cooperative and polite, and firm when necessary
  - Refer to the instructions in your company's dawn raid manual
  - Try to get as much information as possible from the officials in order to find out their concerns
- Make sure officials are accompanied at all times
- Keeping records notes of interview to be checked for accuracy before signing; copying what is copied/removed; notes of search terms; notes of conversations with officials; closing note of the raid
- Ensure that any seals affixed by officials are not broken and that all relevant staff are aware of the existence of seals, especially overnight (e.g. cleaners, contract staff etc.).
   Breaking seals can lead to severe penalties



### Some Dos and Don'ts

### **DON'T**



- Obstruct the officials' investigation: this can lead to severe penalties
- Delete or destroy documents or provide any false or misleading information to officials
- Provide or volunteer to provide additional documents/information to officials and only respond to questions raised
- Give officials original copies (but offer to provide a copy). If original is insisted on then make record of the document taken
- Sign any documents that the officials produce without checking with the Investigation Coordinator or an external lawyer
- Make telephone calls in front of the officials, except where this is unavoidable



# Considerations for potential leniency applicant (1)

Key question: whether or not to seek leniency?

#### **EXPOSURE**

Evidence supporting allegations

- price fixing, customer allocation
- exchange of information

**Duration** 

Fine

**Termination** 

Reputational damage

Other countries' regimes, including criminal

#### COOPERATION

Information available
Added value
Immunity / leniency ranking
Scope of obligation of
cooperation
Exposure to damages actions

#### POTENTIAL DEFENCE

Lines of arguments (legal / factual)
Evidence



# Considerations for potential leniency applicant (2)

#### **SEEK LENIENCY?**

OR NOT?

- Strategic considerations following a dawn raid
  - Criteria to take into account
  - Nature of documents copied during dawn raid
    - 'feeling' that competitor(s) might already have gone in
    - key words used by officials (names, venues etc.)
    - indications given by officials
  - Results of interviews
  - Any lines of defence?



### Document review (1)

- Data collection process
  - Urgent fact-finding required
  - Thorough and systematic review of relevant electronic data essential part of internal investigation
  - Critical considerations include:
    - choice of forensic IT consultant
    - custodian identification
    - filter/search terms
    - organisation of review teams
    - making the results centrally available



### Document review (2)

- Data protection issues
  - Increasingly complex picture: concerns numerous jurisdictions
  - Mainly jurisdiction-specific legal requirements
  - Manage carefully: capable of jeopardising collection process and/or timing
  - Need strategy for complying with relevant obligations:
    - Notify relevant authorities?
    - Obtain consent declarations from custodians?



# Due process: summary of enforcers' powers

	Enforcers (NDRC / SAIC)
Enter business premises	$\checkmark$
Enter residential premises	X
Require production of documents	✓
Require electronic info to be put into electronic format	✓
Forensic imaging of electronic info	✓
Take copies	$\checkmark$
Seize & sift	✓
Legal privilege	X



# Due process: rights of investigated company

#### (1) Privilege against self-incrimination

- In China, only the Criminal Procedure Law prescribes privilege against self-incrimination
- The AML explicitly requires that all the undertakings or individuals being investigated should cooperate with antitrust authorities and must not refuse to be investigated or obstruct the investigation (Article 42)

#### (2) Legal professional privilege

 Certain communications between the undertaking and their lawyers may be protected from disclosure (though not in China, where the concept of privilege is not recognised)

#### (3) Limitation period

 As a general rule, the Chinese authorities may not impose administrative penalties in respect of illegal acts after 2 years (unless otherwise prescribed by law)

#### (4) Right to be heard

 Parties have general right to be informed of the factual and legal basis of the alleged infringement, and general right to submit written defence and request an oral hearing

#### (5) Access to file

- Not explicitly set out in PRC regulations (both antitrust and general)
- No such right for companies under investigation, although theoretically a plaintiff in follow-on damage action may apply with Chinese courts to retrieve files in enforcers' record



### Judicial review

- Challenging the enforcer's decision
  - Companies dissatisfied with enforcer's decision may apply for administrative reconsideration or bring an administrative action
  - Time limits for challenge
    - Administrative reconsideration: within 60 days of decision
    - Administrative litigation: within 3 months of decision
  - Grounds for challenge: infringement of legal rights and interests
  - A decision may be annulled, altered, declared illegal or sent back to the agency for redetermination



### International cooperation

- We are seeing an increase in...
  - Bilateral/multilateral cooperation agreements
  - Active engagement with international competition-related fora to facilitate cooperation and procedural/substantive convergence
  - Dialogue with non-competition institutions (e.g. bribery and corruption)
- Practical implications on companies in a global investigations era
  - Managing multi-jurisdictional issues such as LPP, disclosure obligations, employee rights and data protection
  - Assessing whether leniency and/or settlement are available in each jurisdiction, and the collateral consequences for other jurisdictions
- To facilitate effective international cooperation, authorities should consider:
  - comity and fairness
  - clarity on substantive and procedural rules



# Thank You





